IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Case No. 1:22-CR-123
v.	)	
	)	Honorable Leonie M. Brinkema
EBUKA RAPHAEL UMETI	)	
	)	Trial Date: June 10, 2024
	)	

UNITED STATES' TRIAL BRIEF

The United States of America, by and through its undersigned counsel, hereby files its trial brief to aid the Court in understanding this case and issues that may arise at trial.

I. Statement of the Case

A. The Charges

On August 11, 2022, the Grand Jury returned an Indictment in which it charged the defendant with one count of conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1349 and 3559 (g)(1) (sentencing enhancement); one count of conspiracy to cause intentional damage to a protected computer, in violation of 18 U.S.C. § 371; three counts of wire fraud, in violation of 18 U.S.C. §§ 1343 and 2 (aiding and abetting liability); and one count of intentional damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A)/(c)(4)(B) (sentencing provision) and 2 (aiding and abetting liability). There is also a forfeiture allegation. ECF No. 9. The defendant has pleaded not guilty to all charges and denied the forfeiture allegation.

B. Trial Status

A jury trial is scheduled to begin on June 10, 2024, before the Honorable Leonie M. Brinkema. The United States expects its case-in-chief to last no more than one week.

C. Defense Counsel

The defendant is represented by retained counsel, Charles Burnham.

D. Defendant Custody Status

The defendant is detained in the Alexandria Detention Center.

E. Interpreter

The United States will not require the assistance of an interpreter for any of its witnesses. The defendant also does not require the assistance of an interpreter.

F. Jury Waiver

The defendant has not waived his right to a jury trial.

G. Stipulations

The United States has proposed a number of stipulations, including to images of two laptops and venue. To date, the parties have been unable to agree to any stipulations.

H. Discovery

The United States has complied with its discovery obligations and will continue to do so through and, if applicable, after trial. To date the defendant has not provided any reciprocal discovery, nor filed an exhibit list or provided exhibits to the government. The United States maintains its continuing request for reciprocal discovery.

II. Statement of Facts

Between February 2016 and July 2021, the defendant and his co-conspirators engaged in so-called business email compromise ("BEC") scams. The co-conspirators transmitted phishing emails to victim businesses, which were made to appear as though they originated from trusted individuals, such as a bank or a vendor. These phishing attacks allowed the co-conspirators to gain unauthorized access to victim computer systems and email accounts, including by infecting

victim computers with malware that provided the co-conspirators with remote access. The co-conspirators then exploited that access to obtain sensitive information, which they used to deceive individuals at victim companies into executing wire transfers to accounts specified by the co-defendants. As a result of this scheme, the co-conspirators caused, or attempted to cause, millions of dollars of loss.

As is common in cybercrime cases, the defendant did not engage in all of these activities using his true identity. Instead, he created a variety of accounts using monikers and fake names in an effort to obscure his connection to the crime. However, the defendant did not always fully cover his tracks – in fact, there are numerous instances in which accounts used in the crimes link back to the defendant through both direct and circumstantial evidence. It is anticipated that this attribution evidence – the proof that the defendant was responsible for the intrusions charged in this case – will be the crux of the defense at trial.

Accounts Attributable to the Defendant

The government must therefore prove that the defendant controlled a number of accounts, which link him directly to the charged conspiracy. For example, the defendant's visa application and other personal records were found in a Google account, eternal1502[@]gmail.com. This account was registered under the name "Raphael Raphael," which is the defendant's middle name, repeated twice. The defendant's date of birth is also February 15, which in many countries is listed with the day followed by the month, i.e., 15/02. This eternal1502[@]gmail.com email was used to register an Instagram account – eternal1502 in the name "Raphael" – which contained personal photographs of the defendant. The defendant also used this email address to register a Twitter account – eternal1502 with display name "Raphael." Finally, eternal1502[@]gmail.com was used as a recovery email for another account –

ebuka1502[@]gmail.com. "Ebuka" is the defendant's first name, and the account was registered in the name again of "Raphael Raphael." There is Internet Protocol (IP) address overlap evidence indicating that the eternal1502[@]gmail.com and ebuka1502[@]gmail.com accounts were accessed from the same location, on the same dates, and close in time to one another, which indicates that the two accounts are likely controlled by the same person.

The eternal1502[@]gmail.com account contains a diary-entry style email about the death of the defendant's father sent from jm.collins002[@]gmail.com, another account associated with the defendant. The defendant frequently used "jm.collins" as a moniker. The defendant set up email forwarding rules within the email system of Company B, as alleged in the Indictment, to send copies of emails with certain terms to this jm.collins002[@]gmail.com account. He also sent emails from an employee of Company L, as alleged in the Indictment, which he copied to the jm.collins002[@]gmail.com account.

The defendant sent emails from the jm.collins002[@]gmail.com account to two other email accounts that he controlled – jm.collins100[@]yahoo.com and invoice_s231[@]yahoo.com. A review of the jm.collins100[@]yahoo.com account revealed emails to and/or from victims at Companies A, F, and L, as alleged in the Indictment. A review of the invoice_s231[@]yahoo.com account revealed emails to and/or from individuals at Companies E, F, and G, as alleged in the Indictment.

The invoice_s231[@]yahoo.com account was registered using an alternate email address – helsinki_ar[@]protonmail.com. This email address in turn was used to register a Namecheap account, cassbanks101, in the fictitious persona of "Cassidy Banks." Namecheap is a domain service registrar. The defendant used the cassbanks101 Namecheap account to register a domain name that successfully tricked his victims into believing emails were being sent to or from

Company I, as alleged in the Indictment. The domain he chose used "0" in place of "o" in the company name, a deception that was not revealed unless one viewed the metadata of the relevant emails, which is not something a regular user would ever do. There were also private email subscriptions associated with the cassbanks101 Namecheap account that included a domain similar to that of Company E, except for a minor typographical error, and also Companies F and G, which left the "m" off ".com." These minor changes are again not something that a casual observer of an email would normally notice, and in fact, the individuals sending and receiving emails at Companies I, E, and F did not notice immediately. Finally, in executing his scheme against Company L, as alleged in the Indictment, the defendant caused a malware file on Company L's system to contact a domain – WorldwideTechSecurity.com – which the defendant also registered with the cassbanks101 Namecheap account.

There is also IP address overlap evidence indicating that the jm.collins100[@]yahoo.com and Namecheap cassbanks101 accounts were accessed from the same location, on the same dates, and close in time to one another, which again indicates that they are controlled by the same person.

The defendant used another jm.collins email – jm.collins200[@]icloud.com – to register two Dingtone accounts. Dingtone is a Voice Over Internet Protocol ("VoIP") company, which allows users to make voice calls from a computer, smartphone, or other mobile device. One of these phone numbers ended in 0046 and the other ended in 0057. When the defendant wrote emails impersonating K.H. ("Employee-2" in the Indictment) of Company H, he substituted her real phone number with the 0046 number, which he controlled. Similarly, when the defendant wrote emails to Company K, as alleged in the Indictment, he impersonated a vendor's employee and provided as a contact number the 0057 number, which he controlled. There is IP address

overlap evidence indicating that this Dingtone account and ebuka1502[@]gmail.com account were accessed from the same location, on the same dates, and close in time to one another.

Discord

The defendant used his jm.collins100[@]yahoo.com account to register a Discord account, eternal101. He also used his invoice_s231[@]yahoo.com account to register a ProtonMail account – helsinki-ar[@]protonmail.com – which he in turn used to register a second Discord account, Hels101. Discord is an instant messaging platform, which the defendant and his co-conspirators used to communicate generally about purchasing and effectively using malware. Co-defendant Butaish was the malware creator, while the defendant, co-conspirator Okwonna, and others bought and disseminated Butaish's malware. The Discord chats are full of referrals to Butaish and between the various co-conspirators, as well as Butaish's attempts to advise and improve upon the others' dissemination of that malware. The co-conspirators discussed planning and executing BEC scams, including sharing credentials for accessing compromised computer systems and accounts, accessing compromised email servers, and other hacking tools for executing their schemes.

The co-conspirators also used Discord for more targeted requests. For example, on April 30, 2020, the defendant messaged another user asking for help accessing an email server, "dbschenkey.pw." On May 1, 2020, K.H. (Employee-2 at Company H) received a phishing email via a server located at that same server, "ns1.dbschenkey.pw." Similarly, on May 4, 2020, the defendant messaged another user asking for help accessing an email server, "kirchhof.pw." On the same day, K.H. received a phishing email via a server located at that same server, "kirchhof.pw." As another example, on May 19 and 20, 2020, the defendant purchased access to another email server – "eoncrei.pw" – from another Discord user. On May 21, 2020, L.M. (an

employee of Company L) received a phishing email via a server located at that same server, "eoncrei.pw."

III. Applicable Law

A. Conspiracy to Commit Wire Fraud & Wire Fraud

The defendant is charged in Count One of the Indictment with Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349. This offense has two elements:

(1) two or more persons agreed to commit wire fraud; and

(2) at some time during the conspiracy, the defendant had knowledge of the criminal objective of the agreement and willfully joined the conspiracy with the intent to further its unlawful purpose.

See United States v. Vinson, 852 F.3d 333, 351 (4th Cir. 2017) (citing *United States v. Chittenden*, 848 F.3d 188, 195 (4th Cir. 2017)). There is no overt act requirement. The Indictment also includes an allegation that a statutory sentencing enhancement applies under 18 U.S.C. § 3559(g)(1), namely that the defendant knowingly registered a false domain name and used it in the course of the offense.

The defendant is also charged in Counts Three through Five with Wire Fraud, in violation of 18 U.S.C. § 1343, which is also the object of the conspiracy charged in Count One. This offense also has two elements:

(1) the defendant devised or intended to devise a scheme to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, and promises that were material; and

(2) for the purpose of executing the scheme, the defendant transmitted or caused to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce any writings, signs, signals, pictures, or sounds.

See United States v. Godwin, 272 F.3d 659, 666 (4th Cir. 2001) (identifying two essential elements: (1) a scheme to defraud and (2) use of wire communication in furtherance of the scheme).

"[T]o convict a person of defrauding another, more must be shown than simply an intent to lie to the victim or to make a false statement to him." *United States v. Johnson*, 2022 WL 4376082, at *1 (4th Cir. 2022) (quoting *United States v. Wynn*, 684 F.3d 473, 478 (4th Cir. 2012)). Specifically, "a scheme to defraud 'must be one to deceive the [victim] *and* deprive [him or her] of something of value.'" *Id.* (quoting *Shaw v. United States*, 580 U.S. 63, 72 (2016)); *see also United States v. Skinner*, 2023 WL 2770952, at *1 (4th Cir. 2023) (per curiam) (holding in bankruptcy case that "[s]pecific intent to defraud requires the intent 'to deprive one of something of value through a misrepresentation or other similar dishonest method, which indeed would cause him harm.'" (quoting *Wynn*, 684 F.3d at 478)). As is relevant in this case, communications having a propensity to lull and forestall action on the part of the victim may form an integral part of the overall scheme to defraud. *United States v. Painter*, 314 F.2d 939, 943 (4th Cir. 1963) (citing *United States v. Sampson*, 371 U.S. 75, 80 (1962)).

Furthermore, "[a] misrepresentation is material if 'a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question.'" *United States v. Gillion*, 704 F.3d 284, 296 (4th Cir. 2012) (quoting *Neder v. United States*, 527 U.S. 1, 25 (1999)); *see also Gillion*, 704 F.3d at 297 (upholding jury instructions in mail fraud case that "[a] statement is material if it has a natural tendency to

influence or is capable of influencing the decision-making body to which it was addressed"); *United States v. Lambert*, 2022 WL 2871909, at *3 (4th Cir. July 21, 2022) ("A fact is material if it has a natural tendency to influence or is capable of influencing the intended victim." (quoting *United States v. Pasquantino*, 336 F.3d 321, 333 (4th Cir. 2003) (en banc))).

B. Conspiracy to Cause Intentional Damage to a Protected Computer & Intentional Damage to a Protected Computer

The defendant is charged in Count Two of the Indictment with Conspiracy to Cause Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 371. This offense has three elements:

(1) an unlawful agreement between two or more people to commit a crime;

(2) the defendant 'knowingly and willingly participated in that conspiratorial endeavor'; and

(3) an overt act committed in furtherance of the conspiracy.

Vinson, 852 F.3d at 352 (quoting *United States v. Singh*, 518 F.3d 236, 252 (4th Cir. 2008)).

The defendant is also charged in Count Eleven with Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), which is also the object of the conspiracy charged in Count Two. This offense has four elements:

(1) the defendant caused the transmission of a program, information, code, or command;

(2) the defendant did so knowingly;

(3) as a result of such conduct, the defendant caused damage without authorization to a protected computer; and

(4) the defendant did so intentionally.

See 2A Fed. Jury Prac. & Instr. § 42:15 (6th ed.) (identifying "three essential elements": (1) the defendant knowingly caused the transmission of a program, information, code, or command, to a computer or computer system; (2) the defendant intended to cause damage to a protected computer, computer system, network, information, data, or program; and (3) the damage caused by the defendant was without authorization). The Indictment also includes an allegation that a statutory aggravated penalty applies under 18 U.S.C. § 1030(c)(4)(B), namely that the defendant caused loss to one or more persons during any one-year period aggregating at least $5,000 in value (Counts 2 and 11) or that the offense caused damage affecting ten or more protected computers during any one-year period (Count 2).

As is relevant to this case, a "protected computer" means a computer which is used in interstate or foreign commerce or communication. *See* 18 U.S.C. § 1030(e)(2); *Good 'Nuff Garage, LLC v. McCulley*, 2022 WL 4485810, at *12 (E.D. Va. Sept. 26, 2022) ("Under the CFAA, 'a "[protected] computer" is a high-speed processing device[,] . . . including any data storage facility or communications facility directly related to or operating in conjunction with such device' that 'is used in or affecting interstate or foreign commerce.'" (quoting *WEC Carolina Energy Sol. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012))). "This includes servers and, by extension, accounts connected to the internet requiring authorization credentials for access." *Id.* Generally, "any computer with Internet access" is a "protected computer" and, thus, is "a subject of the [CFAA's] protection." *Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926 (E.D. Va. 2017) (collecting cases).

Damage means any impairment to the integrity or availability of data, a program, a system, or information. *See* 18 U.S.C. § 1030(e)(8). Loss means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and

restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. *See id.* at § 1030(e)(11). As is relevant here, person means any individual, corporation, or other entity. *See id.* at § 1030(e)(12).

C. Venue

Each count alleges two bases for venue in the Eastern District of Virginia: that the defendant was "first brought" here and that some portion of the scheme occurred in this judicial district. "The prosecution bears the burden of proving venue by a preponderance of the evidence[.]" *United States v. Ebersole*, 411 F.3d 517, 524 (4th Cir. 2005). Title 18, United States Code, Section 3238 allows for "trial of all offenses begun or committed . . . out of the jurisdiction of any particular State or district" to be "in the district in which the offender . . . is first brought." Furthermore, 18 U.S.C. § 3237(a) allows for venue "in any district in which such offense was begun, continued or completed[.]" *Ebersole*, 411 F.3d at 525. As to the Conspiracy and Wire Fraud charges in Counts 1 and 3 through 5, the Indictment alleges that emails in furtherance of the scheme to defraud "were sent from or through at least one email server located in the Eastern District of Virginia to locations outside the Commonwealth of Virginia." ECF No. 9 at ¶ 32(e). As to the Conspiracy and Intentional Damage to a Protected Computer charges in Counts 2 and 11, the Indictment alleges that victim Company L "used at least one email server in the Eastern District of Virginia." *Id.* at ¶ 45. In the absence of a stipulation, the government intends to call specific witnesses to prove all forms of alleged venue in this case.

IV. Witnesses

In an abundance of caution, the United States has noticed four witnesses as experts for trial:[1] (1) an employee of Mandiant, noticed as an expert in computer forensic examinations and cyber incident response, who handled the Company E investigation; (2) an employee of Company H, noticed as an expert in computer forensic examinations and cyber incident response; (3) Cary Scardina, the now-retired FBI Special Agent previously assigned to this case, noticed as an expert in the forensic analysis of digital evidence, particularly as it pertains to computer intrusions, account takeover, credential attacks, and malware distribution; and (4) Matthew Hunter, an FBI computer scientist, noticed as an expert in computer forensic examinations. In light of concerns raised by the defendant in a pre-trial motion, the United States has elected to call Cary Scardina as only an expert witness. In preparing for trial, the United States further believes that some of these individuals noticed as experts may not need to be designated at trial as such.

The defendant has not noticed any expert testimony.

The United States intends to call representatives and/or individuals whose accounts were compromised from each of the victim Companies A, B, and E through L. Because co-defendant Okwonna has pleaded guilty, the United States was able to eliminate witness testimony from Companies C and D. The former Chief Financial Officer for Company F has a prior felony conviction for misprision of a felony, which is the subject of a pre-trial ruling limiting the scope of impeachment to the offense and date of conviction and the sentence in the case.

[1] The United States formally noticed five experts, but it was able to excuse one in light of co-defendant Okwonna's guilty plea.

V. Exhibits

The United States anticipates the following general categories of evidence at trial:

A. Business Records

The United States intends to introduce the following business records, all of which are the subject of a pre-trial ruling establishing their authenticity:

Business Record	**Identification of Business Record**	**902(11) Certificate**
Oath (Yahoo) Search Warrant Production for jm.collins100@yahoo.com	Gov. Ex. 100	Gov. Ex. 100A
Oath (Yahoo) Search Warrant Production for invoice_s123@yahoo.com	Gov. Ex. 101	Gov. Ex. 101A
Oath (Yahoo) Subpoena Production for invoice_s123@yahoo.com	Gov. Ex. 101B	Gov. Ex. 101C
NameCheap Search Warrant Production for "Cassidy Banks"/ "cassbanks101"	Gov. Ex. 102	Gov. Ex. 102A
ProtonMail Subpoena Production	Gov. Ex. 104	Gov. Ex. 104A
HackForums Search Warrant Production for eternal101	Gov. Ex. 105	Gov. Ex. 105A
GitHub Subpoena Production for eternal1502	Gov. Ex. 106	Gov. Ex. 106A
Twitter Search Warrant Production for eternal1502	Gov. Ex. 107	Gov. Ex. 107A
Twitter Search Warrant Production for iameternal2	Gov. Ex. 107C	Gov. Ex. 107D
Instagram Search Warrant Production for eternal1502	Gov. Ex. 107F	Gov. Ex. 107G
Google Search Warrant Production for eternal1502@gmail.com	Gov. Ex. 108	Gov. Ex. 108A
Google Subpoena Production for ebuka1502@gmail.com	Gov. Ex. 117	Gov. Ex. 117A
Discord Search Warrant Production for eternal101	Gov. Ex. 109	Gov. Ex. 109A
Discord Search Warrant Production for Hels101	Gov. Ex. 110	Gov. Ex. 110A

Discord Search Warrant Production for Holmes1010	Gov. Ex. 111	Gov. Ex. 111A
Discord Search Warrant Production for Butaish25	Gov. Ex. 112	Gov. Ex. 112A
Apple Subpoena Production for "Raphael Umeti" / eternal1502@gmail.com	Gov. Ex. 113	Gov. Ex. 113A
iCloud Search Warrant Production for jm.collins200@icloud.com	Gov. Ex. 114	Gov. Ex. 114A
Dingtone Subpoena Production for jm.collins200@icloud.com (x0046)	Gov. Ex. 115	Gov. Ex. 115A
Dingtone Subpoena Production for jm.collins200@icloud.com (x0057)	Gov. Ex. 115C	Gov. Ex. 115D
Dingtone Subpoena Production for jm.collins200@icloud.com	Gov. Ex. 115F	Gov. Ex. 115G
Google Search Warrant Production for cass.banks101@gmail.com	Gov. Ex. 116	Gov. Ex. 116A
Google Search Warrant Production for hawlalalam.ali@gmail.com	Gov. Ex. 200	Gov. Ex. 200A
NameCheap Subpoena Production for holmes1010	Gov. Ex. 201	Gov. Ex. 201A
Apple Search Warrant Production for franklin_franklin@icloud.com	Gov. Ex. 203	Gov. Ex. 203A
Company A: Production	Gov. Ex. 300	Gov. Ex. 300A
Company B: Production	Gov. Ex. 400	Gov. Ex. 400A
Company E: Production	Gov. Ex. 600	Gov. Ex. 600A
Company G: Production	Gov. Ex. 700	Gov. Ex. 700A
Company L: Production	Gov. Ex. 1000	Gov. Ex. 1000A
W.B.S.I. Production	Gov. Exs. 1100 & 1100A	Gov. Ex. 1100B
Bitpay Records	Gov. Ex. 1200	Gov. Ex. 1200A

B. Other Records from Victim Companies

The United States also intends to present at trial emails and other records that have not been formally authenticated as business records, but which constitute evidence collected by the victim companies as evidence of the intrusions into their systems. For example, witnesses from

victim companies will testify about emails sent and/or received through their companies' systems during the course of the fraud, many of them through the witness's own email account. "Under [Federal Rule of Evidence] 901, '[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.'" *United States v. Zhu*, 854 F.3d 247, 257 (E.D. Va. 2017) (Ellis, J.) (quoting Fed. R. Evid. 901(a)). "'The burden to authenticate under Rule 901 is not high – only a *prima facie* showing is required.'" *Id.* (quoting *United States v. Vidacak*, 553 F.3d 344, 349 (4th Cir. 2009)). Here, where the proffered emails are illegitimate, the government asserts that these are emails that appear to have been sent or received using victims' legitimate email addresses; the individuals whose legitimate email addresses were misused can identify their own email addresses (or very close approximations thereof) and also confirm that they either did not send or did not receive missives apparently sent from or to their own email accounts. This testimony is sufficient to make the *prima facie* showing that these emails are what the government claims them to be.

Furthermore, these illegitimate emails are either not hearsay or constitute exclusions from the rules against hearsay. First, hearsay requires a "statement," meaning a "person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion." Fed. R. Evid. 801(a). Many of the emails at issue contain no statements at all, and therefore cannot constitute hearsay. Second, hearsay requires that a statement be offered "in evidence to prove the truth of the matter asserted in the statement." Fed. R. Evid. 801(c)(2). The point of offering the fraudulent emails in this case is exactly the opposite, namely that they are untrue. Because these emails are not offered for their truth, they cannot constitute hearsay. Third, a statement offered against an opposing party and "made by the party in an individual . . . capacity" or "made

by the party's coconspirator during and in furtherance of the conspiracy" is not hearsay. Fed. R. Evid. 801(d)(2)(A), (E). Because the government will prove that these emails were crafted either by the defendant himself or by a co-conspirator and sent in furtherance of the conspiracy, they do not constitute hearsay.

Finally, "[a] statement offered for a purpose other than to prove the truth of the assertion contained within the statement is not inadmissible hearsay." *United States v. Guerrero-Damian*, 241 F. App'x 171, 173 (4th Cir. 2007) (citing Fed. R. Evid. 801(c); *United States v. Pratt*, 239 F.3d 640, 643-44 (4th Cir. 2001)). Examples include a statement introduced to "show the effect on the listener[.]" *Id.* (citing *United States v. Safari*, 849 F.2d 891, 894 (4th Cir. 1988)). In this case, the purpose of introducing the illegitimate emails is that they contained false representations that induced a particular, i.e., a material, response from the other party. Introducing them for their effect on the other party means that the statements they contain are not inadmissible hearsay.

C. Summary & Demonstrative Exhibits

The United States anticipates introducing a handful of summary and demonstrative exhibits at trial, including tables created by an individual analyzing the Company H (Gov. Ex. 800T) intrusion; two charts detailing voluminous crypto-currency transactions (Gov. Exs. 1201 and 1202); two charts summarizing the attribution evidence as to the defendant (Gov. Ex. 1400) and co-defendant Okwonna (Gov. Ex. 1401); and a chart summarizing the connections between accounts attributable to the defendant and each intrusion (Gov. Ex. 1402).

Summary and demonstrative exhibits can be used at trial under either Federal Rule of Evidence 611(a)[2] or 1006.[3] The Court has wide discretion under Rule 611(a) to permit summary charts and demonstratives that "facilitate the presentation and comprehension of evidence already in the record." *United States v. Simmons*, 11 F.4th 239, 262 (4th Cir. 2021) (quoting *United States v. Janati*, 374 F.3d 263, 273 (4th Cir. 2004)). Rule 611(a) charts "are not evidence themselves, but are used merely to aid the jury in its understanding of the evidence that has already been admitted" and thus "may include witnesses' conclusions or opinions, or they may reveal inferences drawn in a way that would assist the jury." *Janati*, 374 F.3d at 273. On the other hand, Rule 1006 charts are "admitted into evidence 'as a surrogate for underlying voluminous records that would otherwise be admissible into evidence.'" *Simmons*, 11 F.4th at 262 (quoting *Janati*, 374 F.3d at 273). Because Rule 1006 charts are introduced in lieu of the underlying records, they "must be an accurate compilation of the voluminous records sought to be summarized." *Janati*, 374 F.3d at 272.

---

[2] Rule 611(a) provides:

> (a) Control by the Court; Purposes. The court should exercise reasonable control over the mode and order of examining witnesses and presenting evidence so as to:
> (1) make those procedures effective for determining the truth;
> (2) avoid wasting time; and
> (3) protect witnesses from harassment or undue embarrassment.

[3] Rule 1006 provides:

> The proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court. The proponent must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place. And the court may order the proponent to produce them in court.

The United States anticipates entering Government Exhibit 800T as a summary of voluminous records under Rule 1006 and displaying the remaining exhibits as demonstratives under Rule 611(a).

Rule 1006 Summary of Voluminous Evidence (Gov. Ex. 800T)

Government Exhibit 800T summarizes several emails related to the intrusion at Company H and should be admitted under Rule 1006. The underlying emails from Company H are voluminous, and they are better presented through a summary chart. Government Exhibit 800T briefly summarizes several emails, explaining when they were sent, who sent and received them, and what was in the email. Introducing Government Exhibit 800T as a summary of voluminous writings will increase the efficiency of the trial by serving the core purpose of Rule 1006, "reducing the volume of written documents that are introduced into evidence." *United States v. Oloyede*, 933 F.3d 302, 310 (4th Cir. 2019) (quoting *Janati*, 374 F.3d at 272).

The United States has complied with Rule 1006 by making all the underlying emails available to defense counsel for review. *See* Fed. R. Evid. 1006; *see also Janati*, 374 F.3d at 272–73 ("While [Rule 1006] does not require that the underlying documentation actually be introduced into evidence, it does require that the documents be made available to the opposing party for examination and copying at a reasonable time and place."). By requiring the proponent to make the underlying documents available, Rule 1006 has a built-in "process to test the accuracy of the chart's summarization." *United States v. Blackwell*, 436 F. App'x 192, 199 (4th Cir. 2011). Defense counsel has had both the contents of Government Exhibit 800T and the underlying Company H records either in his possession or available for review since February 2024, and he has not raised an objection or concern with the accuracy of Exhibit 800T. *Cf. id.* (no abuse of discretion in admitting Rule 1006 summary of defendant's telephone calls where

defense did not dispute admissibility of underlying records and did "not suggest that they were deprived of the opportunity to examine the underlying records or challenge the accuracy of the summary in court"). There are no issues with "selectivity" in Government Exhibit 800T, as it does not display certain data for some emails and other data for different emails. *Cf. Oloyede*, 933 F.3d at 310–11 (summary of financial accounts did not satisfy Rule 1006 where different transactions included different categories of information). Instead, Government Exhibit 800T summarizes simple, verifiable information for each relevant email: the date and time, the sender and recipient, whether the email contained fraudulent activity, and a summary of the email's contents.

Rule 611(a) Demonstratives (Gov. Exs. 1201, 1202, 1400, 1401, & 1402)

The United States also expects to present five demonstrative charts under Rule 611(a). Each of these charts will "aid the jury in its understanding of the evidence that has already been admitted." *Janati*, 374 F.3d at 273. Because these demonstratives will not themselves be entered as evidence, they "may include witnesses' conclusions or opinions, or they may reveal inferences drawn in a way that would assist the jury." *Id.* With the large number of witnesses and volume of evidence in this case, Rule 611(a) demonstratives are particularly appropriate given "the length of the trial, the complexity of the case, and the accompanying confusion that a large number of witnesses and exhibits may generate for the jury." *United States v. Johnson,* 54 F.3d 1150, 1159 (4th Cir. 1995). These demonstratives will "aid[] the jury in ascertaining the truth" without unduly prejudicing the defendant. *See id.* (explaining district court should conduct "essentially an analysis under Rule 403" for each Rule 611(a) demonstrative).

Government Exhibits 1201 and 1202 detail voluminous cryptocurrency transactions. Each displays a flow of cryptocurrency through Bitpay, which went toward purchases at NameCheap or eGifter. Without these charts, the jury will have a difficult time understanding

the transaction records from Bitpay and how the FBI was able to draw connections among the Bitpay wallets, registered email addresses, Discord chats, and NameCheap accounts. The underlying records from Bitpay and Namecheap are expected to be previously admitted in evidence as Government Exhibits 109H and 111J (Discord), 102B, 102E, and 201B (NameCheap) and 1200 and 1200B (Bitpay).

Government Exhibits 1400 and 1401 display attribution evidence as to the defendant and Okwonna, respectively. They connect evidence from multiple sources, including Google, Instagram, GitHub, HackForums, Discord, Yahoo!, Namecheap, Apple, AOL, and ProtonMail. The Government expects to display these charts during Special Agent Gerald Kim's testimony, because they properly "reveal inferences drawn in a way that would assist the jury." *Janati*, 374 F.3d at 273. Government Exhibits 1400 and 1401 will aid the jury in understanding Special Agent Gerald Kim's testimony, particularly in light of the voluminous number of exhibits that are expected to be presented during his direct examination. The underlying records are expected to already be in evidence through the 100 and 200 series of the Government's Exhibits.

Finally, Government Exhibit 1402 summarizes the connections between accounts attributable to the defendant and each intrusion. Like Government Exhibits 1400 and 1401, this chart distills a large volume of information—already expected to be in evidence—into a visual format that will assist the jury in understanding the evidence. The information is neutrally presented, without extraneous commentary or information that is unduly prejudicial. Rather, Government Exhibit 1402 simply displays the logo of victim companies alongside email addresses and phone numbers that previous testimony and evidence will have connected to each the intrusion at each company. Like Exhibits 1400 and 1401, this chart is based on information that is expected to be previously admitted into evidence throughout the trial.

VI. Anticipated Trial Issues

The United States flags the following possible concerns for the Court's consideration during trial:

A. Co-Conspirator Statements Made in Furtherance of a Conspiracy

The United States intends to introduce some statements made by the defendant's co-conspirators ("Holmes1010," "Butaish25," and "Deleted User 2d6fc7b," aka "TwistedNerd") in Discord communications. These statements are not hearsay and are admissible against the defendant irrespective of whether the declarant is a current defendant or a non-testifying co-conspirator.

"A statement is not hearsay if it is 'a statement by a co-conspirator of a party during the course and in furtherance of the conspiracy' and is offered against the party." *United States v. Graham*, 711 F.3d 445, 453 (4th Cir. 2013) (quoting Fed. R. Evid. 801(d)(2)(E)). The party offering a co-conspirator's statement must demonstrate by a preponderance of the evidence (1) existence of the conspiracy and (2) that the statement was "during and in furtherance of" the conspiracy. *See Bourjaily v. United States*, 483 U.S. 171, 176 (1987). Whether the offering party has proven the facts by a preponderance of the evidence is a preliminary question for the judge under Federal Rule of Evidence 104(a). *Id.* at 175. To answer that preliminary question, "the court is not bound by evidence rules, except those on privilege." Fed. R. Evid. 104(a). The co-conspirator statement "must be considered but does not by itself establish . . . the existence of the conspiracy or participation in it under (E)." Fed. R. Evid. 801(d)(2).

The Court can consider inadmissible evidence in determining whether Rule 801(d)(2)(E) is satisfied. *See Bourjaily*, 483 U.S. at 178-90. This includes the alleged co-conspirator statement itself. *See, e.g.*, *United States v. Neal*, 78 F.3d 901, 905 (4th Cir. 1996) (citing *United*

States v. Blevins, 960 F.2d 1252, 1255 (4th Cir. 1992) ("[A]n alleged co-conspirator's statements may be considered in determining the existence of the conspiracy.")). The proponent must also offer "independent proof that the co-conspirator declarant was actually in a conspiracy with the defendant challenging the introduction of the statement." *United States v. Dickerson*, 39 F. App'x 850, 861 (4th Cir. 2002).

Here, the United States will establish that the Discord users "eternal101" and "Hels101" are both the defendant, making his statements independently admissible as statements of a party opponent. *See* Fed. R. Evid. 801(d)(2)(A). The "Holmes1010" user is Okwonna, who has already admitted in a Statement of Facts and Plea Agreement entered before this Court that he conspired with the defendant and with Butaish. *See* Dkt. Nos. 66 (Plea Agreement) & 67 (Statement of Facts); *see also Bourjaily*, 483 U.S. at 178-80. The United States can further establish financial relationships between Butaish and the defendant and Okwonna, and it will introduce forensic analysis proving that the defendant and Okwonna worked together to defraud the victim companies using malware created by Butaish.

Finally, the defendant, Butaish, and Okwonna were independently communicating with the same fourth party -- "Deleted User 2d6fc7b" (aka "TwistedNerd") – who specifically told Butaish in June 2020 that "there are 7 of us spreading to the same people," including "hels101, holmes, eternal." Butaish responded: "yeah i know those dudes." *See Neal*, 78 F.3d at 905 (the Court can consider the statement at issue itself); *United States v. Ayala*, 601 F.3d 256, 268 (4th Cir. 2010) ("[I]t is not necessary for the offering party to identify the declarant by name. Instead, the offering party need only 'show' that the unknown declarant was more likely than not a conspirator.'").

"A statement by a co-conspirator is made 'in furtherance' of a conspiracy if it was intended to promote the conspiracy's objectives, whether or not it actually has that effect." *United States v. Shores*, 33 F.3d 438, 443 (4th Cir. 1994). "A particular statement may be found to be 'in furtherance' of the conspiracy even though it is 'susceptible of alternative interpretations' and was not 'exclusively, or even primarily, made to further the conspiracy,' so long as there is 'some reasonable basis' for concluding that it was designed to further the conspiracy." *Id.* at 444 (quoting *United States v. Shoffner*, 826 F.2d 619, 628 (7th Cir. 1987)). In construing the "in furtherance of a conspiracy" language, courts have admitted statements that identify "participants and their roles in the conspiracy," *United States v. Franklin*, 415 F.3d 537, 552 (6th Cir. 2005), or "serve to inform a conspirator of the status of the conspiracy," *United States v. Dawson*, Nos. 95-5146, 95-5342, 95-5152, 95-5187, 1998 WL 188636, at *5 (4th Cir. Apr. 21, 1998) (citing *United States v. Edmond*, 52 F.3d 1080, 1111 (D.C. Cir. 1995)).

At trial, the United States will offer as evidence statements manifestly in furtherance of the charged conspiracies. These statements include discussions about how to improve and execute malware and gaining access to infrastructure necessary to disseminate it. The co-conspirators' statements conveying information regarding the crimes charged in the Indictment – including the purposes, participants, and salient details of these crimes – were made in furtherance of the conspiracy. *See United States v. Diaz*, 176 F.3d 52, 85 (2d Cir. 1999); *Franklin*, 415 F.3d at 552. As a result, these non-testimonial, out-of-court statements are plainly admissible under Rule 801(d)(2)(E).

B. Non-Self-Inculpatory Hearsay

As described above, the United States intends to introduce excerpts of the defendant's communications with co-conspirators and statements of those co-conspirators made in

furtherance of the charged conspiracies, but it will object to any attempts by the defendant to elicit any others portions of those Discord communications. The government is free to introduce against the defendant his own statements in accordance with Federal Rule of Evidence 801(d)(2). A defendant may not however, use his own prior statements even where the government introduced only incriminating portions of them. *See Williamson v. United States*, 512 U.S. 594, 600-601 (1994).

Nor does the "rule of completeness" allow the defendant to introduce portions of his out-of-court statements not offered by the United States. Fed. R. Evid. 106. This rule simply allows an adverse party to require that other admissible evidence be introduced at the same time if fairness so requires, particularly to clarify or explain content already admitted, or prevent the jury from being misled. *United States v. Hassan*, 742 F.3d 104, 134 (4th Cir. 2014). However, "the rule of completeness does not 'render admissible . . . evidence which is otherwise inadmissible under the hearsay rules.'" *Id.* (quoting *United States v. Lentz*, 524 F.3d 501, 526 (4th Cir. 2008)). "Nor does the rule of completeness 'require the admission of self-serving, exculpatory statements made by a party which are being sought for admission by that same party.'" *Id.*

C. Instagram Images for "eternal1502" and Rule 403

Through Government Exhibit 107I, the United States plans to introduce images from the Instagram account "eternal1502," which tend to show that the defendant controlled the Instagram account and other accounts with the "eternal1502" moniker. The United States expects that the defendant will object to the admission of Government Exhibit 107I on the basis that it violates Federal Rule of Evidence 403. These images should be admitted because they are highly

relevant to identify the defendant as involved in the fraudulent scheme and not unduly prejudicial.

Evidence is relevant if it "ha[s] any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence," Fed. R. Evid. 401, and generally, "[r]elevant evidence is admissible," Fed. R. Evid. 402. However, "[t]he court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." Fed. R. Evid. 403.

Rule 403 is a limited remedy. *See United States v. Udeozor*, 515 F.3d 260, 264–65 (4th Cir. 2008) ("Rule 403 is a rule of inclusion, generally favoring admissibility."). "Rule 403 only requires suppression of evidence that results in unfair prejudice—prejudice that damages an opponent for reasons other than its probative value . . . ." *United States v. Mohr*, 318 F.3d 613, 619–20 (4th Cir. 2003). "[D]amage to a defendant's case is not a basis for excluding probative evidence because evidence that is highly probative invariably will be prejudicial to the defense." *United States v. Tillmon*, 954 F.3d 628, 643 (4th Cir. 2019) (quoting *United States v. Basham*, 561 F.3d 302, 326 (4th Cir. 2009)). "[R]elevant evidence should only be excluded under Rule 403 as unfairly prejudicial if there exists 'a genuine risk that the emotions of a jury will be excited to irrational behavior, and this risk is disproportionate to the probative value of the offered evidence.'" *United States v. Williams*, 445 F.3d 724, 730 (4th Cir. 2006) (quoting *United States v. Aramony*, 88 F.3d 1369, 1378 (4th Cir. 1996)).

Courts routinely overrule Rule 403 objections and admit photographs that tend to identify the defendant. Photos tying the defendant to an alias are one example. In *United States v. Luck*,

200 F. App'x 263, 266 (4th Cir. 2006), the district court did not abuse its discretion by admitting three photographs of the defendant over his Rule 403 objection. The photographs depicted several individuals and "were relevant insofar as they matched images of [the defendant] with his alias, C4. Thus, the pictures supported the testimony of [three witnesses], who all referred to [the defendant] and C4 as the same man." *Id.* at 266. The photos were also not unduly prejudicial, because no one was "seen in the photographs possessing narcotics or firearms" and the government "did not attempt to link the phrases [written on the photographs] with the crimes charged." *Id.* Photos of the defendant are also admissible to show his control of areas where the photos are found, which again is relevant to identity. In *United States v. Lewis*, 449 F. App'x 266, 268 (4th Cir. 2011), photos of the defendant with large sums of money were admissible in a drug trafficking and felon-in-possession trial. The photos "were found on the walls of the house in which [the defendant] was staying and tended to show that [the defendant] had a strong connection to the house, making it more likely that the evidence found on the property belonged to him." *Id.*

Photos can also withstand a Rule 403 challenge where they are relevant to both identity and motive. In *United States v. Forrest*, 429 F.3d 73, 79 (4th Cir. 2005), the district court did not abuse its discretion in admitting a photo collection that contained images of a child victim along with pornographic and nonpornographic images of adult males. Despite a Rule 403 objection that the images portrayed the defendant as "as a homosexual, with the prejudice and possible connotation of a child molester as well," the images were highly relevant because they "directly rebutted" defense theories. *Id.* at 79–80. In particular, the images showed that the defendant—not someone else—manufactured the album, because some of the images in the collection were also found in the defendant's home. *Id.* at 80. Additionally, although the defendant claimed he

took photos of the victim to defend himself in a lawsuit, "[t]he images' placement in the album also contradicted the notion that they were taken for innocent, investigatory purposes because [the defendant] inserted them in the album next to pictures showing the same region of the victim's anatomy." *Id.*

These cases all support the admission of Government Exhibit 107I to provide identity and motive, especially where, as here, the defense theory of the case is that the defendant was not responsible for the offense conduct. Here, the photographs in Government Exhibit 107I depict the defendant and come from the "eternal1502" Instagram account, which tends to tie the defendant to that account. The "eternal1502" Instagram account was registered using the email eternal1502[@]gmail.com. That Gmail account received an email from a "jm.collins" account, and the "jm.collins" moniker is directly associated with numerous accounts associated with the fraudulent conduct at the heart of this trial. As in *Forrest*, the photos in Government Exhibit 107I will also rebut any suggestion that someone other than the defendant controlled the "eternal1502" account, or that there is some "innocent" use of the "eternal1502" alias. Furthermore, as this is a fraud case, evidence related to the defendant's high standard of living, which is captured in the contested photographs, is relevant to his motive to steal and attempt to steal millions of dollars.

Finally, these images will not unduly prejudice the defendant. Government Exhibit 107I is highly probative, but "evidence that is highly probative invariably will be prejudicial to the defense." *Tillmon*, 954 F.3d at 643. That is not enough to exclude the photographs under Rule 403 when they are directly relevant to the issues to be litigated at trial.

D. Reciprocal Discovery

This Court may exclude evidence that a defendant failed to produce pursuant to his discovery obligations. Fed. R. Crim. P. 16(d)(2) ("[T]he court may . . . prohibit the party from introducing evidence not disclosed[.]"); *see also Taylor v. Illinois*, 484 U.S. 400, 415 (1988) (defendant's failure to comply with, or object to, government's discovery request before trial justified exclusion of unproduced evidence). The United States has formally requested discovery from the defendant pursuant to Federal Rule of Criminal Procedure 16 in each discovery production letter. To date, the defendant has produced no reciprocal discovery. Should the defendant intend to introduce any other evidence subject to reciprocal discovery, the government again requests that the defense provide the government with such discovery. Otherwise, the government will ask that the Court exclude such evidence pursuant to Rule 16(d)(2).

A defendant cannot avoid his discovery obligation by withholding production until after the government presents its case. A defendant is required to produce all material, pursuant to Rule 16(b), including that which is already in the government's possession and that which the defendant intends to use during the cross-examination of government witnesses. *See United States v. Hsia*, 2000 WL 195067, at *1-2 (D.D.C., Jan. 21, 2000); *United States v. Lin Lyn Trading, Ltd.*, 911 F. Supp. 494, 498 (D. Utah 1996). Indeed, a court may exclude evidence offered by the defense which should have been, but was not, produced under Rule 16(b)(1)(A). *See United States v. Scholl*, 166 F.3d 964, 972 (9th Cir.1999) (upholding exclusion of nine cashier's checks in tax prosecution); *United States v. Hardy*, 586 F.3d 1040, 2044 (6th Cir. 2009) (upholding exclusion of check stub copies in tax evasion case where defendant failed to timely turn it over to the government pretrial); *United States v. Rodriguez Cortes*, 949 F.2d 532, 546 (1st Cir. 1991) (upholding exclusion of phone receipt and letter from defense's case); *United*

States v. Aceves-Rosales, 832 F.2d 1155, 1157 (9th Cir. 1987) (affirming district court's order excluding evidence because defense counsel made a strategic decision to wait until close of government's case to disclose existence of material subject to reciprocal discovery obligations, noting that "[counsel] and his client must accept the risk arising from this behavior").

VII. Conclusion

In this brief, the United States has summarized some of the issues that may arise at trial. Should any additional issues arise, the United States respectfully requests leave to submit such further briefing as may be necessary.

Respectfully submitted,

Jessica A. Aber
United States Attorney

By: /s/
Laura D. Withers
Assistant United States Attorney
Eastern District of Virginia
Thomas S. Dougherty
Trial Attorney
Computer Crime and Intellectual Property Section